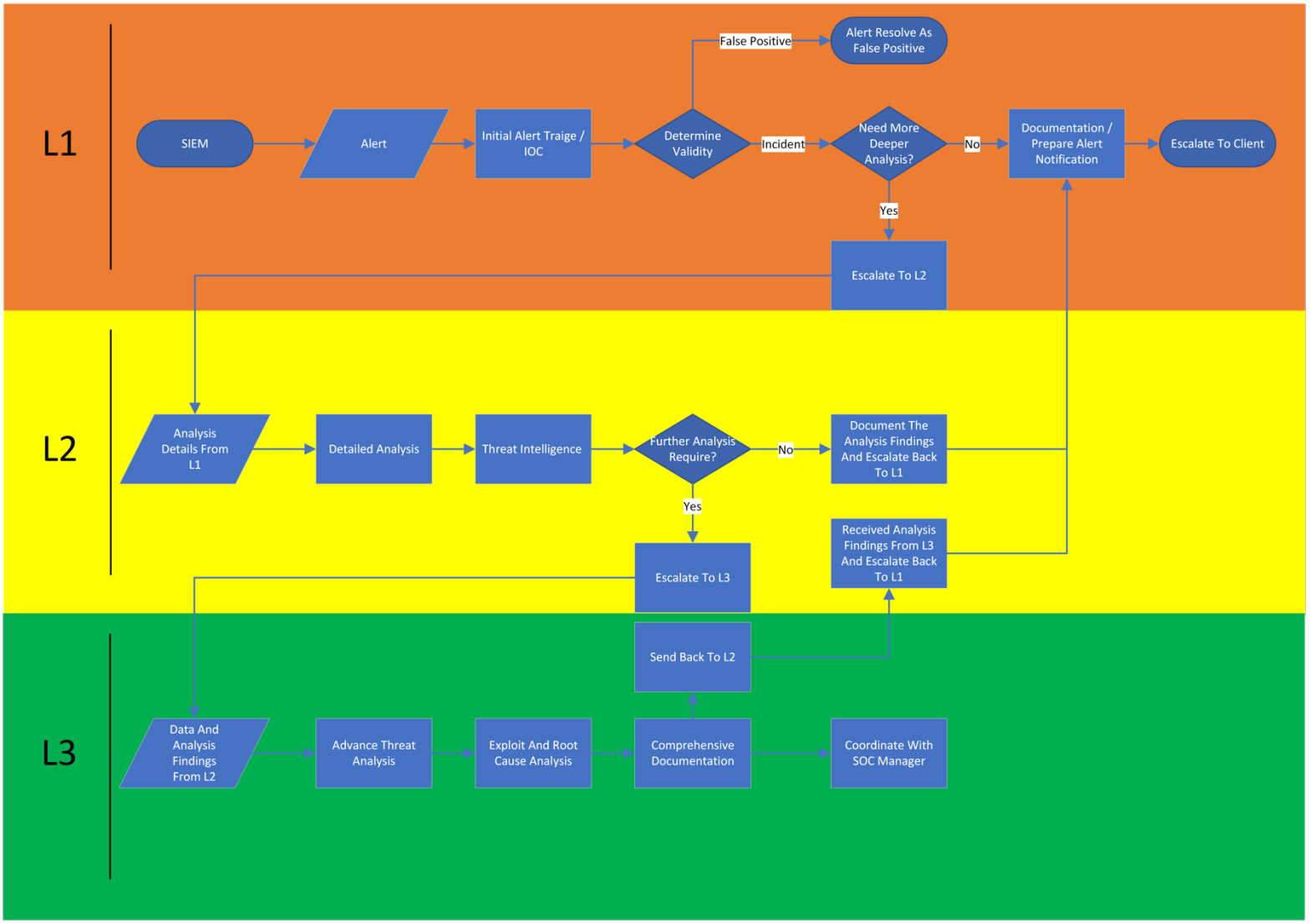
SECURITY OPERATIONS CENTRE (SOC) WORKFLOW WITH EXAMPLES AND SIMULATIONS

BY IZZMIER IZZUDDIN

WORKFLOW


L1
SIEM
Alert
Initial Alert Traige / IOC
Determine Validity
False Positive
Alert Resolve As False Positive
Incident
Need More Deeper Analysis?
No
Documentation / Prepare Alert Notification
Escalate To Client
Yes
Escalate To L2
L2
Analysis Details From L1
Detailed Analysis
Threat Intelligence
Further Analysis Require?
No
Document The Analysis Findings And Escalate Back To L1
Yes
Escalate To L3
Received Analysis Findings From L3 And Escalate Back To L1
L3
Send Back To L2
Data And Analysis Findings From L2
Advance Threat Analysis
Exploit And Root Cause Analysis
Comprehensive Documentation
Coordinate With SOC Manager

BREAKDOWN OF SECURITY OPERATIONS CENTER (SOC) WORKFLOW

Workflow Stages:

1. **L1 Analyst (Tier 1)**
2. **L2 Analyst (Tier 2)**
3. **L3 Analyst (Tier 3)**
4. **SOC Manager**

1. L1 Analyst (Tier 1)

Responsibilities:

- Initial alert triage and validation
- Basic analysis and correlation
- Escalation to L2 if needed

Workflow:

1. **Alert Reception:**
    - SIEM generates an alert.
2. **Initial Alert Review:**
    - Check alert details (e.g., source IP, destination, activity).
    - Validate alert against known baselines and thresholds.
3. **Correlation with Historical Data:**
    - Review historical logs and past activity for the source.
4. **Determine Validity:**
    - Validate if the alert is a false positive or a genuine incident.
5. **Documentation:**
    - Record findings in the incident management system.
    - Include alert details and initial analysis.
6. **Escalation:**
    - If the incident is confirmed or needs deeper analysis, escalate to L2.
    - Provide all pertinent information for L2 analysis.

2. L2 Analyst (Tier 2)

Responsibilities:

- In-depth analysis and investigation
- Threat intelligence correlation
- Initial containment and response actions
- Escalation to L3 if needed

Workflow:

1. **Receive Escalated Incident:**

    - Receive all data from L1.
2. **Detailed Analysis:**
    - Review logs, network traffic, and endpoint security data.
    - Identify patterns and correlate with known threat intelligence.
3. **Contextual Analysis:**
    - Analyse recent activities related to the affected systems.
    - Look for signs of compromise and related alerts.
4. **Threat Intelligence:**
    - Correlate findings with threat intelligence databases.
    - Identify known indicators of compromise (IOCs).
5. **Additional Checks:**
    - Verify endpoint security logs for signs of unauthorised access or abnormal processes.
6. **Documentation:**
    - Record detailed findings in the incident management system.
    - Include logs, patterns, and threat intelligence correlations.
7. **Initial Response:**
    - Implement containment actions (e.g., isolate endpoints).
    - Inform IT and stakeholders for immediate attention.
8. **Escalation:**
    - If further analysis is required, escalate to L3.
    - Provide all collected data and findings for L3 analysis.

3. L3 Analyst (Tier 3)

Responsibilities:

- Advanced threat analysis and digital forensics
- Malware and exploit analysis
- Root cause analysis and comprehensive response planning
- Strategic recommendations for future prevention

Workflow:

1. **Receive Escalated Incident:**
    - Receive all data and findings from L2.
2. **Advanced Threat Analysis:**
    - Perform digital forensics on memory dumps, disk images, and network traffic.
    - Conduct malware and exploit analysis.
3. **Exploit and Root Cause Analysis:**
    - Analyse how the attack was executed and identify the root cause.
    - Determine the full scope and impact of the attack.
4. **Comprehensive Documentation:**
    - Record in-depth findings in the incident management system.
    - Include forensics, malware analysis, and root cause details.
5. **Strategic Recommendations:**

    - Provide recommendations for immediate remediation and long-term prevention.
    - Suggest improvements to security posture and incident response processes.
6. **Coordination with SOC Manager:**
    - Communicate findings and recommendations.
    - Assist in coordinating the overall response strategy.
7. **Post-Incident Review:**
    - Conduct a review with stakeholders to discuss findings and lessons learned.
    - Implement changes based on recommendations.

4. SOC Manager

Responsibilities:

- Oversight and coordination of the SOC team
- Incident management and response coordination
- Communication with stakeholders and leadership
- Continuous improvement of SOC processes

Workflow:

1. **Incident Oversight:**
    - Monitor ongoing incidents and ensure proper escalation and handling.
2. **Coordination and Communication:**
    - Facilitate communication between SOC team members and stakeholders.
    - Ensure that incident responses are aligned with organisational policies.
3. **Resource Allocation:**
    - Allocate resources and support for incident response activities.
    - Ensure that the SOC team has the necessary tools and training.
4. **Post-Incident Review:**
    - Lead post-incident reviews and debriefs.
    - Ensure that lessons learned are documented and improvements are implemented.
5. **Process Improvement:**
    - Continuously evaluate and improve SOC processes and workflows.
    - Stay updated on the latest threats and best practices in cybersecurity.

EXAMPLES AND SIMULATIONS

Scenario 1: Lateral Movement Detection and Analysis

Alert: Suspicious Lateral Movement Detected

- **Source:** SIEM
- **Description:** Multiple failed and successful login attempts detected on various systems within a short timeframe, indicating potential lateral movement within the network.
- **Severity:** Critical
- **Triggered Rules:**
    - Rule 1: 5 failed login attempts on multiple systems within 10 minutes
    - Rule 2: Successful logins on systems previously not accessed by the user

L1 Analysis

L1 Analyst Workflow:

1. **Receive Alert:**
    - The SIEM has generated an alert for potential lateral movement.
2. **Initial Analysis:**
    - **Check Details:**
        - User: dalot
        - Affected systems: SystemA, SystemB, SystemC
        - Source IP: 192.168.1.10
        - Timestamps: Various within the past 10 minutes
        - Number of failed attempts: 5
        - Successful logins: SystemB, SystemC
3. **Correlate with Historical Data:**
    - **Review Past Login Activity:**
        - Regular login systems: SystemA
        - New systems accessed: SystemB, SystemC
4. **Determine Validity:**
    - Unusual login attempts across multiple systems suggest potential lateral movement.
5. **Document Findings:**
    - **Alert Details:**

      Alert ID: 2001
      User: dalot
      Source IP: 192.168.1.10
      Affected Systems: SystemA, SystemB, SystemC
      Failed Attempts: 5
      Successful Logins: SystemB, SystemC
      Status: Escalated to L2

6. **Escalation:**
    - Escalate to L2 analyst with all pertinent information.

Why L1 Can't Solve the Problem:

- **Skill Limitation:** L1 analysts generally have limited skills and tools. They are primarily responsible for monitoring and initial triage.
- **Scope of Work:** L1 is focused on identifying and validating alerts. The complexity of correlating multiple systems' activities and understanding potential lateral movement tactics typically exceeds their role.

L2 Analysis

L2 Analyst Workflow:

1. **Receive Escalated Incident:**
    - Incident escalated from L1 regarding potential lateral movement.
2. **In-depth Analysis:**
    - **Review Logs:**
        - **Failed Login Attempts:**

          Aug 06 12:00:00 - 192.168.1.10 - Failed login for user dalot on SystemA
          Aug 06 12:01:00 - 192.168.1.10 - Failed login for user dalot on SystemB
          ...
          Aug 06 12:05:00 - 192.168.1.10 - Failed login for user dalot on SystemC

        - **Successful Logins:**

          Aug 06 12:10:00 - 192.168.1.10 - Successful login for user dalot on SystemB
          Aug 06 12:12:00 - 192.168.1.10 - Successful login for user dalot on SystemC

3. **Contextual Analysis:**
    - **Check Recent Activity:**
        - Review any recent alerts or activities related to SystemB and SystemC.
4. **Threat Intelligence:**
    - Search for any known indicators related to the source IP or accessed systems.
    - Findings: Source IP associated with a known APT (Advanced Persistent Threat) group.
5. **Additional Checks:**
    - **Endpoint Security Logs:**

        - Verify if the endpoints (SystemB, SystemC) show any signs of compromise or unusual activity.
        - Findings: Abnormal processes running on SystemB, suspicious PowerShell commands executed on SystemC.
6. **Document Findings:**
    - **Detailed Report:**

      Alert ID: 2001
      User: dalot
      Source IP: 192.168.1.10 (Associated with APT group)
      Affected Systems: SystemA, SystemB, SystemC
      Failed Attempts: 5
      Successful Logins: SystemB, SystemC
      Endpoint Analysis: Abnormal processes on SystemB, suspicious PowerShell on SystemC
      Status: Escalated to L3

7. **Coordinate Response:**
    - Isolate affected systems (SystemB, SystemC) to prevent further lateral movement.
    - Inform IT and relevant stakeholders for immediate attention.
8. **Escalation:**
    - Escalate to L3 with all collected data and findings.

Why L2 Can't Solve the Problem:

- **Tool Limitation:** L2 analysts have more tools and expertise than L1, but advanced digital forensics and malware analysis often require specialised tools and skills.
- **Advanced Threat Analysis:** L2 analysts might identify abnormal activities and potential compromise, but deep-dive investigations like malware reverse engineering or root cause analysis typically need L3 expertise.
- **Coordinated Response:** L2 can isolate systems and coordinate initial responses, but strategic decisions and comprehensive remediation plans are often developed by L3.

L3 Analysis

L3 Analyst Workflow:

1. **Receive Escalated Incident:**
    - Incident escalated from L2 regarding potential lateral movement.
2. **Advanced Threat Analysis:**
    - **Digital Forensics:**
        - Collect and analyse memory dumps, disk images, and network traffic from affected systems.

        - Findings: Evidence of a credential dumping tool used on SystemB, suspicious outbound connections on SystemC.
3. **Malware Analysis:**
    - **Static and Dynamic Analysis:**
        - Analyse any malicious binaries found on the affected systems.
        - Findings: Custom malware linked to the APT group, capable of credential theft and lateral movement.
4. **Root Cause Analysis:**
    - Determine how the attackers initially gained access and moved laterally.
    - Findings: Initial access gained via a spear-phishing email targeting dalot, exploiting a known vulnerability.
5. **Strategic Recommendations:**
    - Implement advanced endpoint detection and response (EDR) solutions.
    - Conduct regular phishing awareness training.
    - Patch vulnerabilities promptly.
    - Enhance network segmentation to limit lateral movement.
6. **Document Findings:**
    - **Comprehensive Report:**

      Alert ID: 2001
      User: dalot
      Source IP: 192.168.1.10 (Associated with APT group)
      Affected Systems: SystemA, SystemB, SystemC
      Failed Attempts: 5
      Successful Logins: SystemB, SystemC
      Endpoint Analysis: Abnormal processes on SystemB, suspicious PowerShell on SystemC
      Malware Analysis: Custom malware linked to APT group
      Root Cause: Spear-phishing email, known vulnerability exploited
      Recommendations: Implement EDR, phishing training, patching, network segmentation
      Status: Closed with action items

7. **Post-Incident Review:**
    - Conduct a post-incident review with all stakeholders to discuss findings and recommendations.
    - Implement changes based on the strategic recommendations to prevent similar incidents in the future.

Why L3 Is Necessary:

- **Advanced Skills:** L3 analysts possess advanced skills in digital forensics, malware analysis, and incident response planning.
- **Specialised Tools:** They have access to specialised tools for deep-dive analysis and threat hunting.

- **Comprehensive Analysis:** They can perform root cause analysis, determine the full scope of an attack, and provide strategic recommendations to prevent future incidents.

Scenario 2: Data Exfiltration via Steganography

Alert: Unusual Data Transfer Detected

- **Source:** SIEM
- **Description:** Large data transfers to an external server detected, with suspicious patterns indicating possible steganographic techniques.
- **Severity:** Critical
- **Triggered Rules:**
    - Rule 1: Large outbound data transfer exceeding 1GB within a short timeframe
    - Rule 2: Unusual traffic patterns to an unrecognised external IP

L1 Analysis

L1 Analyst Workflow:

1. **Receive Alert:**
    - The SIEM has generated an alert for unusual data transfer activity.
2. **Initial Analysis:**
    - **Check Details:**
        - Source IP: 192.168.2.50
        - Destination IP: 203.0.113.10
        - Data transferred: 1.2GB
        - Timestamps: Various within the past 15 minutes
3. **Correlate with Historical Data:**
    - **Review Past Data Transfer Activity:**
        - Regular data transfers: Typically less than 100MB, recognised external IPs
        - Current alert: Unrecognised external IP, unusually large data transfer
4. **Determine Validity:**
    - Large data transfer to an unrecognised external IP is suspicious.
5. **Document Findings:**
    - **Alert Details:**

      Alert ID: 3001
      Source IP: 192.168.2.50
      Destination IP: 203.0.113.10
      Data Transferred: 1.2GB
      Status: Escalated to L2

6. **Escalation:**
    - Escalate to L2 analyst with all pertinent information.

Why L1 Can't Solve the Problem:

- **Skill Limitation:** L1 analysts lack the expertise to identify sophisticated data exfiltration techniques such as steganography.
- **Tool Limitation:** They typically do not have access to the specialised tools required for advanced data analysis.

L2 Analysis

L2 Analyst Workflow:

1. **Receive Escalated Incident:**
    - Incident escalated from L1 regarding unusual data transfer.
2. **In-depth Analysis:**
    - **Review Logs:**
        - **Data Transfer Details:**

          Aug 06 12:00:00 - 192.168.2.50 - 203.0.113.10 - 1.2GB transferred

3. **Contextual Analysis:**
    - **Check Recent Activity:**
        - Review any recent alerts or activities related to 192.168.2.50.
4. **Endpoint Security Logs:**
    - Verify if the endpoint (192.168.2.50) shows any signs of compromise or unusual activity.
    - Findings: Multiple large file accesses, network anomalies.
5. **Document Findings:**
    - **Detailed Report:**

      Alert ID: 3001
      Source IP: 192.168.2.50
      Destination IP: 203.0.113.10
      Data Transferred: 1.2GB
      Endpoint Analysis: Multiple large file accesses, network anomalies
      Status: Escalated to L3

6. **Coordinate Response:**
    - Isolate the affected endpoint (192.168.2.50) to prevent further data exfiltration.
    - Inform IT and relevant stakeholders for immediate attention.
7. **Escalation:**
    - Escalate to L3 with all collected data and findings.

Why L2 Can't Solve the Problem:

- **Advanced Threat Analysis:** L2 analysts might identify abnormal activities and potential compromise, but advanced techniques like steganography require L3 expertise.
- **Specialised Tools:** L2 analysts may lack access to tools for deep-dive steganographic analysis.

- **Comprehensive Response:** L2 can isolate systems and coordinate initial responses, but strategic decisions and comprehensive remediation plans are often developed by L3.

L3 Analysis

L3 Analyst Workflow:

1. **Receive Escalated Incident:**
    - Incident escalated from L2 regarding unusual data transfer.
2. **Advanced Threat Analysis:**
    - **Digital Forensics:**
        - Collect and analyse memory dumps, disk images, and network traffic from the affected endpoint.
        - Findings: Evidence of steganographic techniques used to hide data within images and videos.
3. **Steganography Analysis:**
    - **Static and Dynamic Analysis:**
        - Analyse files transferred for hidden data using steganographic tools.
        - Findings: Sensitive data hidden within seemingly benign files.
4. **Root Cause Analysis:**
    - Determine how the attackers managed to use steganography for data exfiltration.
    - Findings: Insider threat using legitimate access to hide data and transfer it.
5. **Strategic Recommendations:**
    - Implement data loss prevention (DLP) solutions.
    - Enhance monitoring for steganographic techniques.
    - Conduct insider threat awareness training.
    - Review and tighten access controls to sensitive data.
6. **Document Findings:**
    - **Comprehensive Report:**

      Alert ID: 3001
      Source IP: 192.168.2.50
      Destination IP: 203.0.113.10
      Data Transferred: 1.2GB
      Endpoint Analysis: Evidence of steganography
      Steganography Analysis: Sensitive data hidden within files
      Root Cause: Insider threat
      Recommendations: Implement DLP, steganography monitoring, insider threat training, access controls review
      Status: Closed with action items

7. **Post-Incident Review:**

    - Conduct a post-incident review with all stakeholders to discuss findings and recommendations.
    - Implement changes based on the strategic recommendations to prevent similar incidents in the future.

Why L3 Is Necessary:

- **Advanced Skills:** L3 analysts possess advanced skills in digital forensics, malware analysis, and incident response planning.
- **Specialised Tools:** They have access to specialised tools for deep-dive analysis and threat hunting.
- **Comprehensive Analysis:** They can perform root cause analysis, determine the full scope of an attack, and provide strategic recommendations to prevent future incidents.

Scenario 3: Advanced Persistent Threat (APT) Detection via DNS Tunneling

Alert: Unusual DNS Queries Detected

- **Source:** SIEM
- **Description:** A high volume of unusual DNS queries detected, indicating potential DNS tunneling activity.
- **Severity:** Critical
- **Triggered Rules:**
  - Rule 1: Excessive DNS queries from a single endpoint
  - Rule 2: DNS queries to domains with abnormal patterns

L1 Analysis

L1 Analyst Workflow:

1. **Receive Alert:**
   - SIEM generates an alert for unusual DNS query activity.
2. **Initial Analysis:**
   - **Check Details:**
     - Source IP: 192.168.3.45
     - Destination Domain: example-malicious-domain.com
     - Number of DNS queries: 500+ within the past hour
3. **Correlate with Historical Data:**
   - **Review Past DNS Activity:**
     - Regular DNS query volume: Typically less than 50 per hour
     - Current alert: Excessive DNS queries to a suspicious domain
4. **Determine Validity:**
   - High volume of DNS queries to an abnormal domain is suspicious.
5. **Document Findings:**
   - **Alert Details:**

     Alert ID: 4001
     Source IP: 192.168.3.45
     Destination Domain: example-malicious-domain.com
     DNS Queries: 500+
     Status: Escalated to L2

6. **Escalation:**
   - Escalate to L2 analyst with all pertinent information.

Why L1 Can't Solve the Problem:

- **Skill Limitation:** L1 analysts typically lack the expertise to recognise sophisticated techniques like DNS tunneling.
- **Tool Limitation:** L1 analysts may not have access to specialised tools required for deeper DNS analysis.

L2 Analysis

L2 Analyst Workflow:

1. **Receive Escalated Incident:**
   - Incident escalated from L1 regarding unusual DNS query activity.
2. **In-depth Analysis:**
   - **Review Logs:**
     - **DNS Query Details:**

       Aug 06 12:00:00 - 192.168.3.45 - example-malicious-domain.com - 500+ queries

3. **Contextual Analysis:**
   - **Check Recent Activity:**
     - Review any recent alerts or activities related to 192.168.3.45.
4. **Threat Intelligence:**
   - Search for any known indicators related to the suspicious domain.
   - Findings: The domain is linked to a known APT group using DNS tunneling for C2 (Command and Control) communication.
5. **Additional Checks:**
   - **Endpoint Security Logs:**
     - Verify if the endpoint (192.168.3.45) shows any signs of compromise or unusual activity.
     - Findings: Suspicious outbound connections and abnormal process activity.
6. **Document Findings:**
   - **Detailed Report:**

     Alert ID: 4001
     Source IP: 192.168.3.45
     Destination Domain: example-malicious-domain.com
     DNS Queries: 500+
     Endpoint Analysis: Suspicious outbound connections, abnormal process activity
     Status: Escalated to L3

7. **Coordinate Response:**
   - Isolate the affected endpoint (192.168.3.45) to prevent further DNS tunneling activity.
   - Inform IT and relevant stakeholders for immediate attention.
8. **Escalation:**
   - Escalate to L3 with all collected data and findings.

Why L2 Can't Solve the Problem:

- **Advanced Threat Analysis:** L2 analysts might identify abnormal activities and potential compromise, but advanced techniques like DNS tunneling require L3 expertise.
- **Specialised Tools:** L2 analysts may lack access to tools for deep-dive DNS and network traffic analysis.
- **Comprehensive Response:** L2 can isolate systems and coordinate initial responses, but strategic decisions and comprehensive remediation plans are often developed by L3.

L3 Analysis

L3 Analyst Workflow:

1. **Receive Escalated Incident:**
    - Incident escalated from L2 regarding unusual DNS query activity.
2. **Advanced Threat Analysis:**
    - **Digital Forensics:**
        - Collect and analyse network traffic captures from the affected endpoint.
        - Findings: Evidence of DNS tunneling for C2 communication.
3. **Malware Analysis:**
    - **Static and Dynamic Analysis:**
        - Analyse any malicious binaries found on the affected endpoint.
        - Findings: Custom malware linked to the APT group, utilizing DNS tunneling for stealthy C2 communication.
4. **Root Cause Analysis:**
    - Determine how the attackers initially gained access and established DNS tunneling.
    - Findings: Initial access gained via a spear-phishing email exploiting a zero-day vulnerability.
5. **Strategic Recommendations:**
    - Implement advanced network monitoring and DNS logging solutions.
    - Conduct regular phishing awareness training.
    - Patch vulnerabilities promptly.
    - Enhance network segmentation to limit the spread of malicious activities.
6. **Document Findings:**
    - **Comprehensive Report:**

      Alert ID: 4001
      Source IP: 192.168.3.45
      Destination Domain: example-malicious-domain.com
      DNS Queries: 500+
      Endpoint Analysis: Suspicious outbound connections, abnormal process activity
      DNS Analysis: Evidence of DNS tunneling for C2 communication
      Malware Analysis: Custom malware linked to APT group
      Root Cause: Spear-phishing email, zero-day vulnerability exploited

Recommendations: Implement advanced network monitoring, phishing training, patching, network segmentation
Status: Closed with action items

7. **Post-Incident Review:**
    - Conduct a post-incident review with all stakeholders to discuss findings and recommendations.
    - Implement changes based on the strategic recommendations to prevent similar incidents in the future.

Why L3 Is Necessary:

- **Advanced Skills:** L3 analysts possess advanced skills in digital forensics, malware analysis, and incident response planning.
- **Specialised Tools:** They have access to specialised tools for deep-dive analysis and threat hunting.
- **Comprehensive Analysis:** They can perform root cause analysis, determine the full scope of an attack, and provide strategic recommendations to prevent future incidents.

Scenario 4: Zero-Day Exploit Detection and Response

Alert: Suspicious Exploit Activity Detected

- **Source:** SIEM
- **Description:** Suspicious exploit activity detected on a critical server, indicating a potential zero-day attack.
- **Severity:** Critical
- **Triggered Rules:**
  - Rule 1: Unusual exploit activity patterns
  - Rule 2: Access to critical files and system configurations

L1 Analysis

L1 Analyst Workflow:

1. **Receive Alert:**
   - SIEM generates an alert for suspicious exploit activity on a critical server.
2. **Initial Analysis:**
   - **Check Details:**
     - Source IP: 192.168.4.75
     - Affected Server: CriticalServer1
     - Exploit Activity: Attempt to access sensitive configuration files
3. **Correlate with Historical Data:**
   - **Review Past Activity:**
     - Regular access patterns: Legitimate user access only
     - Current alert: Unusual exploit activity
4. **Determine Validity:**
   - Exploit activity on a critical server is highly suspicious.
5. **Document Findings:**
   - **Alert Details:**

     Alert ID: 5001
     Source IP: 192.168.4.75
     Affected Server: CriticalServer1
     Exploit Activity: Access to sensitive configuration files
     Status: Escalated to L2

6. **Escalation:**
   - Escalate to L2 analyst with all pertinent information.

Why L1 Can't Solve the Problem:

- **Skill Limitation:** L1 analysts typically lack the expertise to identify and respond to zero-day exploits.
- **Tool Limitation:** L1 analysts may not have access to specialised tools required for deeper exploit analysis.

L2 Analysis

L2 Analyst Workflow:

1. **Receive Escalated Incident:**
    - Incident escalated from L1 regarding suspicious exploit activity.
2. **In-depth Analysis:**
    - **Review Logs:**
        - **Exploit Activity Details:**

          Aug 06 12:00:00 - 192.168.4.75 - CriticalServer1 - Attempt to access sensitive configuration files

3. **Contextual Analysis:**
    - **Check Recent Activity:**
        - Review any recent alerts or activities related to CriticalServer1.
4. **Threat Intelligence:**
    - Search for any known indicators related to the suspicious activity.
    - Findings: The activity matches patterns of a new zero-day exploit recently disclosed.
5. **Additional Checks:**
    - **Endpoint Security Logs:**
        - Verify if the affected server shows any signs of compromise or unusual activity.
        - Findings: Abnormal processes running and unauthorised changes to system configurations.
6. **Document Findings:**
    - **Detailed Report:**

      Alert ID: 5001
      Source IP: 192.168.4.75
      Affected Server: CriticalServer1
      Exploit Activity: Access to sensitive configuration files
      Endpoint Analysis: Abnormal processes, unauthorised configuration changes
      Status: Escalated to L3

7. **Coordinate Response:**
    - Isolate the affected server (CriticalServer1) to prevent further exploit activity.
    - Inform IT and relevant stakeholders for immediate attention.
8. **Escalation:**
    - Escalate to L3 with all collected data and findings.

Why L2 Can't Solve the Problem:

- **Advanced Threat Analysis:** L2 analysts might identify abnormal activities and potential compromise, but advanced techniques like zero-day exploit analysis require L3 expertise.
- **Specialised Tools:** L2 analysts may lack access to tools for deep-dive exploit and system analysis.
- **Comprehensive Response:** L2 can isolate systems and coordinate initial responses, but strategic decisions and comprehensive remediation plans are often developed by L3.

L3 Analysis

L3 Analyst Workflow:

1. **Receive Escalated Incident:**
    - Incident escalated from L2 regarding suspicious exploit activity.
2. **Advanced Threat Analysis:**
    - **Digital Forensics:**
        - Collect and analyse memory dumps, disk images, and network traffic from the affected server.
        - Findings: Evidence of a zero-day exploit compromising the server.
3. **Exploit Analysis:**
    - **Static and Dynamic Analysis:**
        - Analyse any malicious binaries found on the affected server.
        - Findings: Custom exploit code exploiting a zero-day vulnerability in the server software.
4. **Root Cause Analysis:**
    - Determine how the attackers managed to exploit the zero-day vulnerability.
    - Findings: Unpatched software with a known vulnerability, no available patch yet.
5. **Strategic Recommendations:**
    - Implement compensating controls to mitigate the exploit risk.
    - Enhance network monitoring and intrusion detection capabilities.
    - Work with the software vendor to expedite a patch.
    - Conduct a thorough review of all critical servers for similar vulnerabilities.
6. **Document Findings:**
    - **Comprehensive Report:**

      Alert ID: 5001
      Source IP: 192.168.4.75
      Affected Server: CriticalServer1
      Exploit Activity: Access to sensitive configuration files
      Endpoint Analysis: Abnormal processes, unauthorised configuration changes
      Exploit Analysis: Custom exploit code for zero-day vulnerability
      Root Cause: Unpatched software with zero-day vulnerability

Recommendations: Implement compensating controls, enhance monitoring, work with vendor, review critical servers
Status: Closed with action items

7. **Post-Incident Review:**
    - Conduct a post-incident review with all stakeholders to discuss findings and recommendations.
    - Implement changes based on the strategic recommendations to prevent similar incidents in the future.

Why L3 Is Necessary:

- **Advanced Skills:** L3 analysts possess advanced skills in digital forensics, malware analysis, and incident response planning.
- **Specialised Tools:** They have access to specialised tools for deep-dive analysis and threat hunting.
- **Comprehensive Analysis:** They can perform root cause analysis, determine the full scope of an attack, and provide strategic recommendations to prevent future incidents.

Scenario 5: Ransomware Attack with Lateral Movement and Data Encryption

Alert: Ransomware Detected

- **Source:** SIEM
- **Description:** Ransomware detected on multiple endpoints, indicating lateral movement and data encryption.
- **Severity:** Critical
- **Triggered Rules:**
  - Rule 1: Suspicious file encryption activity
  - Rule 2: Multiple failed login attempts followed by successful login

L1 Analysis

L1 Analyst Workflow:

1. **Receive Alert:**
   - SIEM generates an alert for ransomware detected on multiple endpoints.
2. **Initial Analysis:**
   - **Check Details:**
     - Affected Endpoints: 192.168.5.20, 192.168.5.21, 192.168.5.22
     - Ransomware Activity: File encryption detected
3. **Correlate with Historical Data:**
   - **Review Past Activity:**
     - Regular activity: No previous ransomware activity
     - Current alert: Sudden file encryption on multiple endpoints
4. **Determine Validity:**
   - Ransomware activity on multiple endpoints is highly suspicious.
5. **Document Findings:**
   - **Alert Details:**

     Alert ID: 6001
     Affected Endpoints: 192.168.5.20, 192.168.5.21, 192.168.5.22
     Ransomware Activity: File encryption detected
     Status: Escalated to L2

6. **Escalation:**
   - Escalate to L2 analyst with all pertinent information.

Why L1 Can't Solve the Problem:

- **Skill Limitation:** L1 analysts typically lack the expertise to identify and respond to complex ransomware attacks.
- **Tool Limitation:** L1 analysts may not have access to specialised tools required for deeper ransomware analysis.

L2 Analysis

L2 Analyst Workflow:

1. **Receive Escalated Incident:**
    - Incident escalated from L1 regarding ransomware detected on multiple endpoints.
2. **In-depth Analysis:**
    - **Review Logs:**
        - **Ransomware Activity Details:**

          Aug 06 12:00:00 - 192.168.5.20, 192.168.5.21, 192.168.5.22 - File encryption detected

3. **Contextual Analysis:**
    - **Check Recent Activity:**
        - Review any recent alerts or activities related to the affected endpoints.
4. **Threat Intelligence:**
    - Search for any known indicators related to the ransomware activity.
    - Findings: The activity matches patterns of a known ransomware variant with lateral movement capabilities.
5. **Additional Checks:**
    - **Endpoint Security Logs:**
        - Verify if the affected endpoints show any signs of compromise or unusual activity.
        - Findings: Unauthorised login attempts, abnormal process activity, and data encryption.
6. **Document Findings:**
    - **Detailed Report:**

      Alert ID: 6001
      Affected Endpoints: 192.168.5.20, 192.168.5.21, 192.168.5.22
      Ransomware Activity: File encryption detected
      Endpoint Analysis: Unauthorised login attempts, abnormal process activity
      Status: Escalated to L3

7. **Coordinate Response:**
    - Isolate the affected endpoints to prevent further ransomware spread.
    - Inform IT and relevant stakeholders for immediate attention.
8. **Escalation:**
    - Escalate to L3 with all collected data and findings.

Why L2 Can't Solve the Problem:

- **Advanced Threat Analysis:** L2 analysts might identify abnormal activities and potential compromise, but advanced techniques like lateral movement and data encryption analysis require L3 expertise.

- **Specialised Tools:** L2 analysts may lack access to tools for deep-dive ransomware and network traffic analysis.
- **Comprehensive Response:** L2 can isolate systems and coordinate initial responses, but strategic decisions and comprehensive remediation plans are often developed by L3.

L3 Analysis

L3 Analyst Workflow:

1. **Receive Escalated Incident:**
    - Incident escalated from L2 regarding ransomware detected on multiple endpoints.
2. **Advanced Threat Analysis:**
    - **Digital Forensics:**
        - Collect and analyse memory dumps, disk images, and network traffic from the affected endpoints.
        - Findings: Evidence of ransomware with lateral movement capabilities, encrypting files and demanding ransom.
3. **Ransomware Analysis:**
    - **Static and Dynamic Analysis:**
        - Analyse any malicious binaries found on the affected endpoints.
        - Findings: Custom ransomware variant using advanced evasion techniques and lateral movement.
4. **Root Cause Analysis:**
    - Determine how the attackers managed to deploy ransomware and move laterally.
    - Findings: Initial access gained via a compromised user account, followed by lateral movement and deployment of ransomware.
5. **Strategic Recommendations:**
    - Implement advanced endpoint detection and response (EDR) solutions.
    - Enhance network segmentation to limit lateral movement.
    - Conduct regular ransomware awareness training.
    - Review and tighten access controls to sensitive systems.
6. **Document Findings:**
    - **Comprehensive Report:**

      Alert ID: 6001
      Affected Endpoints: 192.168.5.20, 192.168.5.21, 192.168.5.22
      Ransomware Activity: File encryption detected
      Endpoint Analysis: Unauthorised login attempts, abnormal process activity
      Ransomware Analysis: Custom variant with lateral movement
      Root Cause: Compromised user account, lateral movement, ransomware deployment
      Recommendations: Implement EDR, network segmentation, ransomware training, access control review

Status: Closed with action items

7. **Post-Incident Review:**
    - Conduct a post-incident review with all stakeholders to discuss findings and recommendations.
    - Implement changes based on the strategic recommendations to prevent similar incidents in the future.

Why L3 Is Necessary:

- **Advanced Skills:** L3 analysts possess advanced skills in digital forensics, malware analysis, and incident response planning.
- **Specialised Tools:** They have access to specialised tools for deep-dive analysis and threat hunting.
- **Comprehensive Analysis:** They can perform root cause analysis, determine the full scope of an attack, and provide strategic recommendations to prevent future incidents.